

1
2
3
4
5
6
7
8 **UNITED STATES DISTRICT COURT**
9 **CENTRAL DISTRICT OF CALIFORNIA**

10
11 OCEAN S., et al.

12 Plaintiffs,

13 v.
14

15 LOS ANGELES COUNTY, et al.,

16 Defendants.
17

)
) CASE NO. 2:23-cv-06921-JAK-E
)

) **STIPULATED ORDER RE:**
) **DISCOVERY OF**
) **ELECTRONICALLY STORED**
) **INFORMATION**
)
)
)
)

1 **1. GENERAL PROVISIONS**

2 1. This Order will govern discovery of electronically stored information
3 (“ESI”) in this case.

4 2. The parties are aware of the importance the Court places on cooperation
5 and commit to meet and confer in good faith throughout the matter consistent with this
6 Court’s Standing Order on Discovery Disputes, the Federal Rules of Civil Procedure,
7 and the Local Rules of this Court. The parties acknowledge that they have reviewed
8 and shall reference the Court’s Checklist for Conference of Counsel Regarding ESI
9 during any Rule 26 conference and when seeking to resolve discovery disputes about
10 ESI during meet-and-confer conferences.

11 3. The parties have identified liaisons to each other who are and will be
12 knowledgeable about and responsible for discussing their respective ESI. Each e-
13 discovery liaison will be, or have access to those who are, knowledgeable about the
14 technical aspects of e-discovery, including the location, nature, accessibility, format,
15 collection, search methodologies, and production of ESI in this matter. The parties will
16 rely on the liaisons, as needed, to confer about ESI and to help resolve disputes without
17 court intervention.

18 4. To the extent reasonably practicable, the production of documents shall be
19 conducted in a manner that facilitates efficient access to documents and minimizes
20 related discovery costs. The terms of this Order shall be construed so as to ensure the
21 prompt, efficient, and cost-effective exchange of information consistent with the
22 Federal Rules of Civil Procedure, this Court’s Civil Standing Order, the Local Rules of
23 the Central District of California, and any other orders by this Court.

24 5. Except as specifically limited herein, this Order governs the production of
25 discoverable documents by the parties and third-parties to the litigation.

26 6. This Order shall not enlarge, reduce, or otherwise affect the scope of
27 discovery in this litigation as imposed by Federal Rules of Civil Procedure, this
28 Court’s Civil Standing Order, the Local Rules of the Central District of California, and

1 any other orders by this Court, nor imply that discovery produced under the terms of
2 this Order is properly discoverable, relevant, or admissible in this or in any other
3 litigation.

4 7. Nothing in this Order shall be interpreted to require disclosure of
5 materials that a party contends are not discoverable or are protected from disclosure by
6 the attorney-client privilege, the attorney work product doctrine, or any other privilege
7 that may be applicable. Additionally, nothing in this Order shall be deemed to waive
8 or limit any Party's right to object to the production of certain electronically stored
9 information, or to move for an appropriate protective order on the ground that the
10 sources are not reasonably accessible because of undue burden or cost or otherwise.

11 8. The Parties agree to alert all other Parties concerning any technical
12 problems associated with complying with this Order. To the extent compliance with
13 this Order imposes an unanticipated, undue burden with respect to any protocol stated
14 herein, the parties shall promptly confer in an effort to resolve the issue.

15 9. Consistent with their obligations under the Federal Rules of Civil
16 Procedure, this Court's Civil Standing Order, and the Local Rules of the Central
17 District of California, the parties will attempt to resolve disputes regarding the issues
18 set forth herein prior to filing a motion with the Court, or otherwise seeking relief. If
19 the Parties are unable to resolve the dispute after a good faith effort, the parties may
20 seek Court intervention in accordance with the Court's procedures.

21 **2. KEYWORD SEARCHES**

22 1. For voluminous ESI such as emails that can be most efficiently searched
23 for responsive documents using keyword searches, the Parties agree to conduct
24 keyword searches using search terms that have been reasonably calculated in good
25 faith to retrieve responsive ESI. Within one week following the transmittal of the first
26 document production that used ESI searches in response to a request for production,
27 the producing party shall disclose:

28 a. the search terms it applied to the overall collected materials to

1 retrieve responsive ESI (regardless of whether the first production includes ESI using
2 all of the search terms or only a subset thereof);

3 b. the custodians and document repositories (e.g., shared drives,
4 databases, wikis) searched (regardless of whether the first production includes ESI
5 using all of those custodians and repositories or only a subset thereof);

6 c. any date restrictions applied;

7 d. Any other restrictions (e.g., file types) which would limit the
8 universe of data to which search terms will be applied; and

9 2. If a party producing ESI on a rolling basis modifies its search terms,
10 custodians, document repositories, and date restrictions after any document production,
11 it will disclose those modifications without delay and no later than a week following
12 the transmittal of the next document production. The producing party shall retain the
13 sole right and responsibility to manage and control searches of its data files, including
14 the right to make revisions to the parameters of its document review, in order to make
15 the review more accurate and cost-effective, provided that it will disclose those
16 revisions per above.

17 3. The parties reserve all rights to challenge the adequacy of the search
18 terms, custodians/repositories, and other restrictions that are used by another party to
19 collect responsive ESI using keywords, and contemplate that ESI productions will be
20 completed on a rolling basis in a sufficiently timely manner to leave adequate time for
21 such challenges. If a party believes that a keyword search is inadequate for any of the
22 above reasons, or that discovery has revealed that a supplemental search would be
23 appropriate, the party shall propose the supplemental custodians, repositories, search
24 terms, and/or parameters, and the parties shall meet and confer in good faith about
25 whether such an additional search would be relevant and proportional to the needs of
26 the case. The producing party shall provide a Hit Report with the number of unique
27 records (with and without families) that the search returned, as well as the number of
28 unique records (with and without families) for each term (i.e., returning that term and

1 no others) for the proposed additional search, or explain why such a report would be
2 unduly burdensome or otherwise inappropriate. If the parties reach an impasse as to
3 the requested supplemental search, the requesting party may move to compel. The
4 burden shall be on the moving party to justify its request for additional custodians,
5 repositories, search terms, and/or parameters.

6 **3. TECHNOLOGY-ASSISTED REVIEW**

7 If a producing party elects to apply technology assisted review (“TAR”) for the
8 identification or review of responsive records for production, it shall disclose that to
9 opposing counsel without delay and the parties will meet and confer about the use of
10 TAR, including appropriate disclosures regarding the producing party’s TAR process
11 and the timing of those disclosures. If the parties fail to reach agreement, the receiving
12 party may move to compel additional disclosure about the producing party’s TAR
13 process. Nothing herein restricts a producing party from using TAR to help organize
14 or manage its internal review process, provided, however, that a party using TAR to
15 identify or review documents for production will disclose the same, per above.

16 **3. DEDUPLICATION**

17 Parties will ensure that only exact (bit-by-bit) duplicates are subject to
18 deduplication using industry standard eDiscovery software. Deduplication shall occur
19 at the family rather than file level (*e.g.*, a standalone document that is an exact copy of
20 an email attachment shall not deduplicate).

21 **4. EMAIL THREAD SUPPRESSION**

22 A producing party may use industry-standard email thread suppression to
23 suppress non-inclusive or duplicative messages within email threads, and produce only
24 the unique and/or most complete version of an email thread, consisting of those that
25 are textually unique, include unique attachments, or both. Duplicative emails shall
26 include only those email messages in which the parent document, senders and
27 recipients (including blind copy), and all attachments are exactly the same. If a
28 producing party elects to utilize such email thread suppression for its productions, it

1 shall use industry standard eDiscovery software to do so and disclose the name of the
2 software to receiving Party.

3 **5. PRODUCTION FORMAT**

4 **a) ESI Production Format**

5 Except as provided in Sections 7(d), 7(e), and 9(c), ESI shall be produced
6 electronically, as single page, uniquely and sequentially numbered Group IV TIFF files
7 at 300 dpi resolution, with a corresponding load file (“Image Load File”) and
8 document-level Extracted Text files. For ESI that does not have Extracted Text, a
9 document-level Object Character Recognition (“OCR”) text file shall be created and
10 included, associated with the underlying records, and included in the production. With
11 regard to ESI documents that are redacted for privilege or responsiveness, the images
12 shall be accompanied by OCR text files generated after redaction (thereby excluding
13 the redacted portions from the OCR file). All text files shall be named to match the
14 endorsed number assigned to the image of the first page of the document. The images
15 shall also be accompanied by an “OPT” image cross-reference load file corresponding
16 to the TIFF files, a data load file (“DAT”) providing the beginning and ending
17 endorsed number of each document and the number of pages it comprises, shall
18 contain the metadata associated with each Production Field specified in the Metadata
19 Appendix and suitable for loading into an industry standard litigation database (*e.g.*,
20 Relativity), and shall provide links to document-level text files. Notwithstanding
21 anything to the contrary, all documents shall be produced as they are maintained in the
22 ordinary course of business.

23 **b) Production of Paper Discovery**

24 The producing party shall produce hard-copy documents electronically as
25 scanned, single-page TIFF image format, uniquely and sequentially numbered Group
26 IV TIFF files at 300 DPI resolution, with a corresponding load file (“Image Load
27 File”) and document-level OCR text file, but may provide PDF format when single-
28 page TIFF format is not practicable. With regard to hard copy documents produced

electronically that are redacted for privilege or responsiveness, the images shall be accompanied by document-level OCR text files generated after redaction (thereby excluding the redacted portions from the OCR file). The images shall also be accompanied by an “OPT” image cross-reference load file corresponding to the TIFF files, a data load file (“DAT”) providing the beginning and ending endorsed number of each document and the number of pages it comprises, shall contain the relevant hard copy Production Fields specified in Schedule A and suitable for loading into an industry standard litigation database (*e.g.*, Relativity), and shall provide links to document-level text files. If a hard copy document is more than one page, to the extent possible, the unitization of the document and any attachments or affixed notes shall be maintained as it physically existed when collected by the producing party and shall include appended notes, post-its, coversheets, or labels.

d) Appearance and Content

Subject to any appropriate redactions, each document’s TIFF/JPEG/PDF file shall be a static representation of the contents of the document in its original format, whether paper or electronic. Parties shall make efforts to resolve issues such as imaging or formatting problems or documents that are not reasonably usable in the prescribed form of production. Documents containing color need not be produced in color unless the color lends special context or substance to the document.

e) Production of ESI in Native Format

Parties agree that spreadsheet files (*e.g.*, Microsoft Excel) and multimedia files (*e.g.*, Video or Audio files) shall be produced in their Native Format. In the event that production of other types of documents in TIFF/JPEG/PDF file format would be impracticable or not reasonably usable, the producing party shall produce any other such documents in Native Format. Metadata load file for files produced natively shall contain a link to the produced Native Files, as indicated in APPENDIX A.

f) Databases and Structured Data and Proprietary Systems

Certain data types may be impracticable or not reasonably usable to produce in

1 TIFF/JPEG/PDF or in Native Format. Potential examples include, but are not limited
2 to, structured data stored in a database, documents created in a non-commercially
3 available system or applications that are only meaningful when viewed in the context
4 of that system or application or data created in legacy software that is no longer
5 available. Without imposing or undertaking any obligations in excess of those
6 provided by the Federal Rules of Civil Procedure, the Parties agree to meet and confer
7 with respect to the production of this type of data to determine how such data might be
8 produced in a cost reasonably usable way. For example, structured data in a database
9 might best be produced as static reports from the database.

10 **g) Document Numbers and Confidentiality Designations for Documents**
11 **Produced as Images**

12 Each page of a document produced in TIFF/JPEG/PDF file format shall have a
13 legible, unique fixed-length numeric identifier (“Document Number”) containing at
14 least eight (8) digits electronically overlayed onto the image in no less than 10-point
15 font. Unless it would obscure, conceal or interfere with any information originally
16 appearing on the document, the Document Number shall be overlayed on the lower
17 right hand corner of the document. Unless it would obscure, conceal or interfere with
18 any information originally appearing on the document, any confidentiality designation
19 pursuant to the Stipulated Protective Order entered in this case shall appear on the
20 lower left hand side of each page of a document produced, in no less than 10-pt font.
21 The Document Number for each document shall be created so as to identify the
22 producing party and the Document Number (*e.g.*, “DEF00000001”) and shall not
23 contain spaces. Each producing party shall use a unique identifying name of its choice.

24 **h) Document Numbers and Confidentiality Designations for Documents**
25 **Produced in Native Format**

26 Since Native Format productions are not static and cannot be branded on each
27 page in the same manner as TIFF/JPEG/PDF images, each electronic file produced in
28 Native Format shall be assigned a unique Document Number. The producing party

1 shall include a single-page TIFF/JPEG/PDF image branded with this unique Document
2 Number and the phrase “PRODUCED IN NATIVE FORMAT” branded in the center
3 of the page. To protect the confidentiality of files produced natively, any
4 confidentiality designations pursuant to the Stipulated Protective Order must appear on
5 the TIFF/JPEG/PDF placeholder on the lower left hand corner in no less than 10-point
6 font. Native file names shall be identical to the Document number, followed by the file
7 extension, (*e.g.*, “DEF00000001.xls”). No party may attach to any pleading or any
8 correspondence addressed to the Court, or any adverse or third party, or submit as an
9 exhibit at a deposition or any other judicial proceeding, a copy of any document in
10 Native Format produced by any party without ensuring that the corresponding Bates
11 number and confidentiality legend, as designated by the producing party, appears in
12 the Native File name.

13 **h) Exception Files**

14 The Parties will use reasonable efforts to address Documents that present
15 imaging or form production problems (including encrypted and/or protected files
16 identified during the processing of ESI) (“Exception Files”). Exception Files identified
17 for production will be produced as a Bates-stamped placeholder TIFF/JPEG bearing
18 the legend “This document was unable to be processed.” The parties will meet and
19 confer regarding requests for the production of the native versions of Exception Files.
20 The producing party will undertake reasonable efforts to attempt to make encrypted or
21 password-protected files available. If the Parties cannot reach agreement on the
22 handling of Exception Files through the meet and confer process, the matter may be
23 submitted to the Court for resolution.

24 **i) Hyperlinked Content**

25 The producing party shall produce any responsive, non-privileged, nonpublic
26 hyperlinked content within responsive, non-privileged emails or other collaborative
27 documents (*e.g.*, wikis, SharePoints, etc) solely to the extent such hyperlinked content
28 is itself in the producing party’s possession, custody, or control, and associate such

1 linked content either by treating as a family with appropriate group identifier metadata
2 or via some other metadata that clearly identifies the link between the communication
3 and the hyperlinked file, to the extent practicable.

4 **l) Parent-Child Relationships**

5 Parent-child relationships (defined as the association between an attachment and
6 its parent document or between embedded documents and their parent) shall be
7 preserved.

8 **m) Family Groups**

9 A document and all other documents in its attachment range, emails with
10 attachments, and files with extracted embedded OLE documents all constitute family
11 groups. If any member of a family group is produced, all members of that group must
12 either also be produced or else logged as privileged or withheld based on other
13 enumerated grounds set out in the Protective Order, and no such member shall be
14 withheld from production as a duplicate. No family members shall be withheld from
15 production on relevance grounds, other than for the specific grounds enumerated in the
16 Protective Order. If a member of a family group is withheld from production under a
17 privilege objection and that document is later determined not to be privileged, the
18 document shall then be produced with metadata that links it to the family group from
19 which it was originally withheld.

20 **6. REDACTIONS AND PRIVILEGE LOG**

21 1. On a rolling basis within 60 days of each document production, each party
22 shall provide a log of redacted documents in that production..

23 2. On a rolling basis, within 60 days of substantial completion of production
24 in response to any request for production, each party shall provide a log of documents
25 responsive to that request for production but withheld for any reason.

26 3. Notwithstanding the prior two paragraphs, by no later than 60 days before
27 the fact discovery cutoff, each party shall produce a log of all remaining responsive
28 documents it has withheld or redacted.

1 4. Pursuant to Fed. R. Evid. 502(d), the production of a privileged or work-
2 product-protected document, whether inadvertent or otherwise, is not a waiver of
3 privilege or protection from discovery in this case or in any other federal or state
4 proceeding. For example, the mere production of privileged or work-product-protected
5 documents in this case as part of a mass production is not itself a waiver in this case or
6 in any other federal or state proceeding

7 5. Similarly, the production of any personally identifiable information, or
8 other private information, or confidential information does not constitute waiver of
9 those rights, privileges, and protections, whether inadvertent or not.

10 6. Documents and communications involving litigation counsel need not be
11 logged.

12 7. If a party believes that a document-by-document privilege log is infeasible
13 for a particular category of documents other than communications involving litigation
14 counsel, the parties will meet and confer about the scope and content of a categorial
15 privilege log for those documents.

16 **7. THIRD PARTY SUBPOENAS**

17 A Party that issues a non-party subpoena (the “Issuing Party”) must include a
18 copy of this Order with the subpoena and request that the non-party produce
19 documents in accordance with the specifications set forth herein.

20 The Issuing Party is responsible for producing, without modification or
21 exclusion, any documents obtained pursuant to a non-party subpoena to all other
22 parties.

23 If the non-party production is not Bates-stamped, the Issuing Party will brand
24 the non-party production images with unique prefixes and Bates numbers, or otherwise
25 identify Native Files before producing them to the other parties, per the technical
26 specifications outlined in this Order’s Protocol.

27 Nothing in this Order is intended to, or may be interpreted as, narrowing,
28 expanding, or otherwise affecting either the rights of the Parties or of any non-parties

1 to object to a subpoena.

2 **8. MODIFICATION**

3 This Stipulated Order may be modified by a Stipulated Order of the parties or by
4 the Court for good cause shown, including but not limited to, if compliance with this
5 Stipulated Order proves unduly burdensome, impracticable, disproportionate,
6 unreasonably expensive, leads to undue delay, interferes with governmental
7 functioning, or is otherwise unreasonable in practice. Nothing in this Stipulated Order
8 waives these rights.

9 **9. INFORMATION SECURITY AND PRIVACY**

10 1. Upon discovery or reasonable belief of any unauthorized access, use,
11 modification, exposure, acquisition, disclosure, compromise, or loss of County, DCFS
12 or State Defendants' data and information ("Security Incident"), the County and State
13 Defendants shall be notified no later than (48) hours. Breach reports of shall include, to
14 the extent available, the identification of everyone whose Data has been, or is
15 reasonably believed to have been accessed, viewed, acquired, or disclosed during such
16 breach.

17 2. When storing or transferring any electronic data or information covered
18 by this Order to or from a cloud-based environment, the parties must ensure that the
19 ESI is fully encrypted, with AES 256-bit encryption, and must make a good-faith effort
20 to ensure the ESI is not disclosed or made available to any unauthorized party.

21 3. All ESI covered by this Order shall be stored on document storage media
22 encrypted with AES 256-bit encryption, and kept in a location that is not accessible to
23 any unauthorized party.

24 4. The parties shall take reasonable steps to: (a) prevent unauthorized public
25 disclosure or dissemination of any information covered by this Order; and (b) establish
26 and maintain reasonable and appropriate measures and safeguards to prevent such
27 unauthorized disclosure or dissemination. This includes measures to promptly
28 identify, detect, defend, respond to, mitigate, and prevent any unauthorized acquisition,

1 access, use, alteration, disclosure, loss, or damage of due to any cause, whether
2 intentional, accidental, manmade, or natural. A receiving party who is or becomes
3 aware of a disclosure covered by this paragraph shall notify the producing party
4 thereof within 24 hours of its discovery.

5
6
7 Dated: November 4, 2024

8 By: /s/ Grant A. Davis-Denny

9 Grant A. Davis-Denny
10 Munger, Tolles & Olson LLP
11 350 South Grand Avenue, Fiftieth Floor
12 Los Angeles, California 90071-3426
13 Telephone: (213) 683-9100
Facsimile: (213) 687-3702
Attorney for Plaintiffs

14 Dated: November 4, 2024

15 By: /s/ Farbod S. Moridani

16 Farbod S. Moridani (SBN 251893)
17 fmoridani@millerbarondess.com
18 Miller Barondess, LLP
19 2121 Avenue of the Stars, Suite 2600
Los Angeles, California 90067
Telephone: (310) 552-4400
Facsimile: (310) 552-8400
Attorney for County Defendants

20 Dated: November 4, 2024

21 By: /s/ Andrew Z. Edelstein

22 Andrew Z. Edelstein
23 andrew.edelstein@doj.ca.gov
24 California Department of Justice
25 300 S Spring St, Ste 1702
26 Los Angeles, CA 90013-1256
Deputy Attorney General
Attorney for State Defendants

27 **IT IS ORDERED** that the forgoing Agreement is **APPROVED**.
28



1 Dated: 11/5/24

2 CHARLES F. EICK
3 UNITED STATES MAGISTRATE JUDGE
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

METADATA APPENDIX

Field	Definition	Record Type
BEGBATES	Beginning Bates Number (production number).	All
ENDBATES	Ending Bates Number (production number).	All
BEGATTACH	First Bates number of family range, i.e. Bates number of the first page of the parent e-mail or document.	Email, eDocuments
ENDATTACH	Last Bates number of family range, i.e. Bates number of the last page of the last attachment or, if no attachments, the document itself.	Email
PGCOUNT	Number of pages in the document.	All
HASHVALUE	MD5 hash value.	All
ALLCUSTODIANS	List of all persons or data sources from where documents/files are produced; values delimited by semi-colon.	All
FILESIZE	File Size.	All

Field	Definition	Record Type
FILEPATH	Original file/path of the location where the item was located at the time of collection. This should include location, file name, and file extension. Any container name should be included in the path.	eDocuments
FILENAME	Original file name at the point of collection.	eDocuments
EXTENSION	File extension.	All
EMAILID	Email system identifier assigned by the host email system. This value is extracted from parent message during processing.	Email
EMAILSUBJECT	Subject line of email.	Email
EMAILFROM	Email sender.	Email
EMAILTO	Email recipient.	Email
EMAILCC	Additional email recipients.	Email
EMAILBCC	Blind, additional email recipients.	Email
TITLE	Document title as assigned by	eDocuments
AUTHOR	Creator of a document.	eDocuments
LASTMODIFIEDBY	Last person/user who modified or saved a document.	eDocuments
DATECREATED (mm/dd/yyyy hh:mm:ss)	Creation Date and Time.	eDocuments

Field	Definition	Record Type
DATELASTMODIFIED (mm/dd/yyyy hh:mm:ss AM)	Date and Time Last Modified.	eDocuments
DATESENT (mm/dd/yyyy hh:mm:ss AM)	Date and Time the email was sent.	Email
IMPORTANCE	Indication of Priority of E-mail message.	Email
REDACTION	Indicator for documents that have been redacted. PRIVILEGED for Privilege redactions, PII for Personal Identifying Information redactions.	All
CONFIDENTIALITY	Confidentiality level as assigned pursuant to any applicable Protective Order or stipulation to match branding on the face of production image.	All
EXCEPTION	“Y” or “Yes” for documents that were processing or extractions exceptions, blank/null if not present.	All
NATIVEFILELINK	For documents provided in native format only.	All
TEXTPATH	File path for OCR or Extracted Text files.	All